UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/042,019	01/08/2002	Zheng Qi	BRCMP007/BP-1687	4910

7590 04/07/2006

CHRISTIE, PARKER & HALE, LLP
P.O. BOX 7068
PASADENA, CA 91109-7068

EXAMINER	
COLIN, CARL G	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 04/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/042,019	QI, ZHENG	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 1/20/2006, applicant adds claims 23-24 and amends claims 1, 6, 8, 10, and 15. The following claims 1-24 are presented for examination.

2. Applicant's remarks, pages 14-20, filed on 1/20/2006, with respect to the rejection of claims 1-22 have been fully considered but they are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3.1 Claims 23-24 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim contains subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Applicant's disclosure fails to recite the limitations recited in the added dependent claims 23-24

as claimed. "a multiplexer to select an output of the combined adder tree of claim 1" and "performing a multiplexing operation to provide an output of the combined adder tree of claim 10" respectively.

Double Patenting

4. A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the conflicting claims so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

4.1 Claims 1, 4-10, 12-17, and 19-22 are provisionally rejected under 35 U.S.C. 101 as claiming the same invention as that of claims 1-31 of copending Application No. 09/827,882. For instance, claim 1 of the present application is drawn to identical subject matter as claim 8 of the copending Application No. 09/827,882. Claim 10 of the present application is drawn to identical subject matter as claim 8 of the copending Application No. 09/827,882. This is a provisional double patenting rejection since the conflicting claims have not in fact been patented.

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 2, 3, 11, 18, and 23-24 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 2, 8, and 23 of copending Application No. 09/827,882 in view of non-Patent Literature "An Efficient Implementation of Hash Function Processor for IPSEC" to Kang et al. Regarding claim 2, Kang et al discloses a way to minimize the adder delay by implementing adder, multiplexer operation, and CLA. Therefore, it would have been obvious to one of ordinary skill in the art to modify the architecture disclosed in the copending application to use a hash round logic implementation with a timing critical path equivalent to one of: 5-bit addition, one 32-bit CSA, a multiplexer operation, and one-32 bit CLA and three 32-bit CSAs, a multiplexer operation, and one-32 bit CLA as suggested by Kang et al in order to minimize delay in the timing critical path in performing SHA-1 authentication algorithm.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

6.1 **Claims 1, 3, 5, 10, 12, 16, and 23-24** are rejected under 35 U.S.C. 102(a) as being anticipated by non-Patent Literature "An Efficient Implementation of Hash Function Processor for IPSEC" to Kang et al, pp. 1-4.

6.2 **As per claim 1**: Kang et al discloses an authentication engine architecture for a SHA-1 multi-round authentication algorithm, comprising: a hash engine configured to implement hash round logic for an SHA1 authentication algorithm, the hash round logic implementation including, a combined adder tree with a timing critical path having a single 32-bit carry look-ahead adder (CLA) (see pages 1-2, sections 2-3).

As per claim 10: Kang et al discloses receiving a data packet stream; splitting the packet data stream into fixed-size data blocks (see section 2.3); and processing the fixed-size data blocks using a SHA-1 multi-round authentication engine architecture, said architecture implementing hash round logic for a SHA1 authentication algorithm including a combined adder tree with a timing critical path having a single 32-bit carry look-ahead adder (CLA) (see section 2.1-3.2).

As per claims 3 & 12: Kang et al discloses the limitation of wherein the additions performed by the combined adder tree are preceded by a 5-bit circular shifter (see fig. 2).

As per claims 5 & 16: Kang et al discloses the limitation of wherein the combined adder tree is configured such that addition computations are conducted in parallel with round operations (section 3.1).

As per claims 23 & 24: Kang et al discloses a multiplexer and carry select adder for seslecting output of combined adder tree that meets the recitation of comprising a multiplexer to select an output of the combined adder tree and comprising performing a multiplexing operation to provide an output of the combined adder tree.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7.1 **Claims 2, 4, 6, 7, and 11** are rejected under 35 U.S.C. 103(a) as being unpatentable over non-Patent Literature "An Efficient Implementation of Hash Function Processor for IPSEC" to Kang et al, pp. 1-4.

As per claims 2, 4, & 11: Kang et al discloses a timing critical path equivalent to one of: 5-bit addition, one 32-bit CSA, a multiplexer operation, and one-32 bit CLA and three 32-bit CSAs, a

multiplexer operation, and one-32 bit CLA and further discloses the combined adder tree includes add5to1 and add4to1 adders (see sections 3.1-3.3 and figs. 2-3 and 5). It is apparent to one of ordinary skill in the art that the number of registers or bits may be chosen as a matter of design choice because it only requires routine skill in the art to modify the architecture to use different numbers of adders bits, or multiplexers.

As per claim 6: Kang et al discloses the authentication engine architecture of claim 1, wherein the architecture is implemented as an authentication engine architecture for a multi-loop, SHA-1 authentication algorithm comprising: a first instantiation of a SHA-1 authentication algorithm hash round logic in an inner hash engine (see sections 3.1-3.3 and figs. 2-5); a second instantiation of an SHA-1 authentication algorithm hash round logic in an outer hash engine (see sections 3.1-3.3 and figs. 2-5); a dual-frame payload data input buffer configured for loading one new data block while another data block one is being processed in the inner hash engine (see sections 3.1-3.3 and figs. 2-5); an initial hash state input buffer configuration for loading initial hash states to the inner and outer hash engines for concurrent inner hash and outer hash operations (see sections 3.1-3.3 and figs. 2-5); and a dual-ported ROM configured for concurrent constant lookups for both inner and outer hash engines (see sections 3.1-3.3 and figs. 2-5). Kang et al discloses an architecture configured for parallel processing and two separate input buffers. Although not explicitly stated loading one new data block while another data block one is being processed in the inner hash engine, as the term parallel processing is well known in the art, it is apparent to one of ordinary skill in the art that Kang et al's architecture is configured to perform parallel processing such as loading one new data block while another data block one is being

processed. Therefore, it would have been obvious to one of ordinary skill in the art to load one new data block while another data block one is being processed to save in processing time by performing parallel processing as suggested by Kang et al.

As per claim 7: Kang et al discloses the authentication engine architecture of claim 6, wherein the multi-loop, multi-round authentication algorithm is HMAC-SHA1 (see section 1).

8. **Claims 8-9, 13-15, 17-22** are rejected under 35 U.S.C. 103(a) as being unpatentable over non-Patent Literature "An Efficient Implementation of Hash Function Processor for IPSEC" to Kang et al, pp. 1-4 as applied to claim 1 above, in view of Schneier "Applied Cryptography, Second Edition", John Wiley & Sons, New York, 1996, Pages 436-445.

As per claims 8-9, 13, 14, 15, & 17: Kang et al discloses five hash state registers; and discloses implementing parallel processing (figure 2) and using one path that is not a critical path as illustrated in figs. 2-4, thereby collapsed the number of rounds that meets the recitation of wherein eighty rounds of an SHA1 loop are collapsed into forty rounds (see sections 2.1-3.2 and figs. 2-4). Kang et al does not explicitly state one critical and four non-critical data paths associated with the five registers, such that in successive SHA1 rounds, registers having the critical path are alternative because Kang et al they are well known or inherent features of the architecture disclosed. However, in figures 2 and 5 such feature can be shown. Schneier in an analogous art teaches the basic concept of SHA that providing more detailed explanation and discloses one critical and four non-critical data paths associated with the five registers, such that

in successive SHA1 rounds, registers having the critical path are alternative (Pages 442-445). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to apply Schneier concept of secure hash algorithm description that is well known in the art in the system of Kang et al. One of ordinary skill in the art would have been motivated to do so in order to ensure the security of the messages being sent and exchanged in the system and save in processing time (Page 442).

As per claim 18: Kang et al discloses wherein the multi-loop, multi-round authentication algorithm is HMAC-SHA1 (see section 1).

As per claims 19-22: claims 20-22 recite similar limitation as found in claim 6. Claim 19 recites similar limitation as found in claims 6, 9, and 13 as per pipelining or parallel processing of operations with inner and outer hash engine. Therefore, these claims are rejected on the same rationale as the rejection of claims 6, 9, and 13.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses some of the claimed features such as parallel processing, reducing rounds, reducing critical path, etc.

US Patents: 5,940,877 Eickemeyer et al ; 5,548,544 Matheny et al ; 5,299,319 Vassiliadis et al.

9.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information As per the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cc

Carl Colin
Patent Examiner
March 30, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER
CR 4/2/06